Theoretical Computer Science 83 (1991) 337-343
Elsevier

Note

On the p-isomorphism conjecture

Osamu Watanabe

Department of Computer Science, Tokyo Institute of Technology, Tokyo 152, Japan

Communicated by P. Young
Received November 1987
Revised February 1990

Abstract

Watanabe, O., on the p-isomorphism conjecture (Note), Theoretical Computer Science 83 (1991) 337-343.

We show, for example, the following claim: if EXPSPACE ($\stackrel{\text{def}}{=}$ DSPACE(2^{poly})) has a non-p-isomorphic pair of complete sets, then it has a complete set that is not p-isomorphic to U and that is of the form $f(U)$ for some one-way function f, where U is any fixed paddable complete set in EXPSPACE. We have similar but weaker results for the class NP, super-polynomial complexity classes, and classes that include co-NEXP.

1. Introduction

By analogy with recursive function theory, Berman and Hartmanis [2] conjectured that all complete sets in NP are p-isomorphic; indeed, they showed that almost all complete sets in NP arising from practical fields satisfy this conjecture. (In this note, by "complete set" we mean "complete set under $\leqslant_m^P$-reducibility".) This conjecture is generalized to any reasonable complexity class $\mathscr{C}$.

Generalized *p*-isomorphism conjecture for $\mathscr{C}$. *All complete sets in $\mathscr{C}$ are* p-*isomorphic.*

The conjecture claims that all complete sets in $\mathscr{C}$ share similar structures. On the other hand, if the conjecture fails, then $\mathscr{C}$ has a *non*-p-*isomorphic complete set*, a complete set that is not p-isomorphic to standard complete sets thus having a structure different from them. In this note, we study the form of such nonstandard complete sets.

Joseph and Young [8] found some complete sets in NP, namely k-creative sets, for which no proof currently exist for showing their p-isomorphism to a standard complete set, say SAT. In other words, k-creative sets are candidates for non-p-isomorphic complete sets in NP. On the other hand, there is a simple candidate for non-p-isomorphic complete sets. Suppose that there exists a one-way function f, i.e., a function that is one-to-one, honest[1], and polynomial-time computable, but is not polynomial time invertible. (Note that it is open to prove such a function exists even from the assumption that $P \neq NP$.) It is easy to show that $f(SAT)$ is complete in NP. On the other hand, there is no reason to expect that $f(SAT)$ should be p-isomorphic to SAT. That is, $f(SAT)$ is also a candidate for non-p-isomorphic sets. In this note, we investigate the question whether such a type of simple complete set exists if the generalized p-isomorphism conjecture fails.

We give an affirmative answer to our question by considering the class NP, super-polynomial complexity classes, and classes including co-NEXP. We can solve our question affirmatively for classes that include co-NEXP and are closed under complement. For example, we have the following claim for the class EXPSPACE: if EXPSPACE has a non-p-isomorphic pair of complete sets, then it has a non-p-isomorphic complete set of the form $f(U)$ for some one-way function f (where U is any fixed standard complete set in EXPSPACE).

We assume that the reader is familiar with the notions and previous works concerning the p-isomorphism conjecture. (The reader will find a good survey on this topic in [4, 8].) The following notions and notations are preliminary to the following discussion.

We use Σ to denote our finite alphabet. For any string x, $|x|$ denotes the length of x. We assume some pairing function $\lambda xy.\langle x, y\rangle$ that is one-to-one, honest, polynomial-time computable, and polynomial-time invertible. For any A and B, let $A \times B$ denote the set $\{\langle a, b\rangle : a \in A \wedge b \in B\}$.

By restricting $\leqslant^{P}_{m}$-reductions, we define the following relations between sets A and B:

- A is $\leqslant^{P}_{1,h}$-*reducible* to B (write $A \leqslant^{P}_{1,h} B$) if A is $\leqslant^{P}_{m}$-reducible to B via a one-to-one and honest reduction f,
- A is $\leqslant^{P}_{inv}$-*reducible* to B (write $A \leqslant^{P}_{inv} B$) if A is $\leqslant^{P}_{1,h}$-reducible to B via a polynomial-tie invertible reduction f, and
- A is *p-isomorphic* to B (write $A \equiv^{P}_{iso} B$) if A is $\leqslant^{P}_{inv}$-reducible to B via a reduction f whose range is Σ^*. (In other words, $A \equiv^{P}_{iso} B$ if $A \leqslant^{P}_{m} B$ via a polynomial-time invertible bijection.)

In order to show the p-isomorphism between given sets, Berman and Hartmanis introduced the concept of *padding function*. A set L is (*polynomially*) *paddable* if $L \times \Sigma^* \leqslant^{P}_{inv} L$. A (*polynomial*) *padding function* for L is a $\leqslant^{P}_{inv}$-reduction from $L \times \Sigma^*$ to L. The following properties are important in this note. (Their proofs are clear from the discussion in [2]; thus, they are omitted.)

[1] A function is called *honest* if there is a polynomial p such that $(\forall x \in \Sigma^*)[|x| \leqslant p(|f(x)|)]$.

Proposition 1. *Consider any complexity class $\mathscr{C}$ that has a paddable complete set U. Let C be any complete set in $\mathscr{C}$.*

(1) $C \leq^{\mathrm{P}}_{\mathrm{inv}} U$.

(2) $U \leq^{\mathrm{P}}_{\mathrm{inv}} C$ *if and only if* $U \equiv^{\mathrm{P}}_{\mathrm{iso}} C$.

(3) C *is paddable if and only if* $U \equiv^{\mathrm{P}}_{\mathrm{iso}} C$.

Finally we clarify our notion of standard complete set and reasonable complexity class. Any well-known complete set in NP, PSPACE, ... is shown to be paddable. Thus, we regard a paddable complete set as a *standard complete set.* A *non* p-*isomorphic complete set* is a complete set that is not p-isomorphic to a standard complete set. We say that a complexity class $\mathscr{C}$ is *reasonable* if (i) it is closed under taking intersections and unions with sets in P, and (ii) it has a paddable complete set. Note that many complexity classes that have been studied in the literature satisfy these conditions.

2. Main results

First we discuss our question on the class NP.

Theorem 1. *Let U be a standard complete set in* NP. *If there exists a non-*p*-isomorphic complete set X in $\mathscr{C}$ and if $U \leq^{\mathrm{P}}_{\mathrm{m}} X$ via some reduction f such that $f(\Sigma^*) \in \mathrm{P}$, then either the set $f(U)$ or the set $\overline{f(\bar{U})}$ is a non-*p*-isomorphic complete set.*

The following lemma provides a simple proof of this theorem.

Lemma 1 (Cole [5, 6]). *Let D, L_1, and L_2 be any sets such that*

(i) $D \in \mathrm{P}$,

(ii) $L_1, L_2 \subseteq D$ *and* $L_1 \cap L_2 = \emptyset$, *and*

(iii) L_1 *and* L_2 *are paddable.*

Then L_1 has a padding function whose range is included in D.

Proof. The reader can easily find the proof in the discussions in [5, 6]. Here we state the outline of the proof. Let π_1 and π_2 be a padding function of L_1 and L_2 respectively. Define π by

$$\pi(\langle x, y\rangle) = \begin{cases} \pi_1(\langle x, y\rangle) & \text{if } \pi_1(\langle x, y\rangle) \in D - \mathrm{Range}(\pi_3), \\ \pi_3(\langle x, y\rangle) & \text{otherwise,} \end{cases}$$

where $\pi_3(\langle x, y\rangle) \stackrel{\mathrm{def}}{=} \pi_2(\langle x_0, \langle x, y\rangle\rangle)$ for some fixed $x_0 \in L_2$. Then it is easy to show that this π satisfies the lemma. □

Proof of Theorem 1. First we show that both $f(U)$ and $\overline{f(\bar{U})}$ are complete sets in NP. Note that $f(U) = X \cap f(\Sigma^*)$ and $\overline{f(\bar{U})} = X \cup \overline{f(\Sigma^*)}$. Thus, both $f(U)$ and $\overline{f(\bar{U})}$

are sets in NP because $f(\Sigma^*) \in \mathrm{P}$ and NP is closed under taking intersections and unions with sets in P. Note that f is a $\leq^{\mathrm{P}}_{\mathrm{m}}$-reduction from U to X; thus, for every $x \in \Sigma^*$, $x \in U \leftrightarrow f(x) \in X$. On the other hand, for every $x \in \Sigma^*$, $f(x) \in X \leftrightarrow f(x) \in f(U)$ $(=X \cap f(\Sigma^*))$ and $f(x) \in \overline{X} \leftrightarrow f(x) \in \overline{f(\bar{U})}$ $(=X \cup \overline{f(\Sigma^*)})$. That is, f witnesses that $U \leq^{\mathrm{P}}_{\mathrm{m}} f(U)$ and $U \leq^{\mathrm{P}}_{\mathrm{m}} \overline{f(\bar{U})}$. Therefore, both $f(U)$ and $\overline{f(\bar{U})}$ are complete sets in NP.

Next we prove that either $U \not\equiv^{\mathrm{P}}_{\mathrm{iso}} f(U)$ or $U \not\equiv^{\mathrm{P}}_{\mathrm{iso}} \overline{f(\bar{U})}$. Assume the contrary that both $f(U)$ and $\overline{f(\bar{U})}$ are p-isomorphic to U. Then it follows from Proposition 1 that both $f(U)$ and $f(\bar{U})$ have a padding function. Let $D = f(\Sigma^*)$, $L_1 = f(U)$, and $L_2 = f(\bar{U})$. From Lemma 1, L_1 $(=f(U))$ has a padding function π whose range is included in D $(=f(\Sigma^*))$. Now define $g(x) = \pi(f(x), x)$. Then for every $x \in \Sigma^*$,

$$
\begin{aligned}
x \in U &\leftrightarrow f(x) \in f(U) && (U \leq^{\mathrm{P}}_{\mathrm{m}} f(U) \text{ via } f)\\
&\leftrightarrow \pi(f(x), x) \in f(U) && (\pi \text{ is padding for } f(U))\\
&\leftrightarrow \pi(f(x), x) \in X && (\mathit{Range}(\pi) \subseteq f(\Sigma^*) \text{ and } f(U) = X \cap f(\Sigma^*))\\
&\leftrightarrow g(x) \in X.
\end{aligned}
$$

That is, $U \leq^{\mathrm{P}}_{\mathrm{m}} X$ via g. Furthermore, from its construction, g is one-to-one and polynomial time invertible. Hence, $U \leq^{\mathrm{P}}_{\mathrm{inv}} X$ via g. Therefore, it follows from Proposition 1 that $U \equiv^{\mathrm{P}}_{\mathrm{iso}} X$. A contradiction. □

We say that a function t is *super-polynomial* if

$$(\forall p\text{: polynomial})(\exists n_0)(\forall n \geq n_0)[p(n) \leq t(n)].$$

A complexity class $\mathscr{C}$ is called *super-polynomial* if $\mathrm{DTIME}(t) \subseteq \mathscr{C}$ for some super-polynomial t. Next we investigate our question on super-polynomial complexity classes.

Theorem 2. *Let $\mathscr{C}$ be a reasonable super-polynomial complexity class that is closed under union, and let U be a standard complete set in $\mathscr{C}$. If there exists a non* p*-isomorphic complete set X in $\mathscr{C}$ and if $U \leq^{\mathrm{P}}_{\mathrm{m}} X$ via some reduction f such that $f(\Sigma^*) \in \mathrm{P}$, then $f(U)$ is a non-*p*-isomorphic complete set in $\mathscr{C}$.*

Proof. Following the same argument as in the proof of Theorem 1, we can prove that $f(U)$ is complete in $\mathscr{C}$. Thus, it suffices to show that $f(U)$ is not p-isomorphic to U.

By way of contradiction, suppose that $U \equiv^{\mathrm{P}}_{\mathrm{iso}} f(U)$. Then $U \leq^{\mathrm{P}}_{\mathrm{inv}} f(U)$ from Proposition 1.

Let t be a super-polynomial such that $\mathrm{DTIME}(t) \subseteq \mathscr{C}$. Since $f(\Sigma^*) \in \mathrm{P}$, there exists a deterministic machine that accepts $f(\Sigma^*)$ within $q(n)$ time for some polynomial q.

Let $\{T_i\}_{i\geq 0}$ be an enumeration of polynomial-time transducers, and let ϕ_i and p_i be the function computed by T_i and a polynomial-time bound for T_i respectively. (We assume that some fixed universal transducer simulates T_i on input w within $|i| \cdot p_i(|w|)^2$steps.)

Now consider the following set $L_f \subseteq \mathrm{N} \times \Sigma^*$:

$$\langle i, x\rangle \in L_f \overset{\text{def}}{\longleftrightarrow} |i| \cdot p_i(|\langle i, x\rangle|)^2 + q \circ p_i(|\langle i, x\rangle|) \leq t(|\langle i, x\rangle|)$$
$$\wedge [\phi_i(\langle i, x\rangle) \notin f(\Sigma^*) \vee x \in U].$$

By using the assumption that (i) $\mathscr{C}$ is a reasonable complexity class, (ii) $\mathrm{DTIME}(t) \subseteq \mathscr{C}$, and (iii) $\mathscr{C}$ is closed under union, it is easy to show that $L_f \in \mathscr{C}$. Thus, it follows from Proposition 1 that $L_f \leq^{\mathrm{P}}_{\mathrm{inv}} U$; hence, $L_f \leq^{\mathrm{P}}_{\mathrm{inv}} f(U)$. Let N_{i_0} be a transducer that computes a $\leq^{\mathrm{P}}_{\mathrm{inv}}$-reduction from L_f to $f(U)$; that is, $L_f \leq^{\mathrm{P}}_{\mathrm{inv}} f(U)$ via ϕ_{i_0}.

Let n_0 be an integer such that

$$(\forall n \geq n_0)[|i_0| \cdot p_{i_0}(n)^2 + q \circ p_{i_0}(n) \leq t(n)].$$

Consider any input $z = \langle i_0, x\rangle$ such that $n_0 \leq |z|$. Then we have $\phi_{i_0}(z) \in f(\Sigma^*)$. Otherwise, $z \in L_f$ (from the definition of L_f) and $\phi_{i_0}(z) \notin f(U)$ (since $f(U) \subseteq f(\Sigma^*)$), which contradicts that ϕ_{i_0} is a reduction from L_f to $f(U)$. Thus, for every x such that $n_0 \leq |\langle i_0, x\rangle|$,

$$\begin{aligned} x \in U &\leftrightarrow \langle i_0, x\rangle \in L_f && (\text{since } \phi_{i_0}(\langle i_0, x\rangle) \in f(\Sigma^*)) \\ &\leftrightarrow \phi_{i_0}(\langle i_0, x\rangle) \in f(U) && (\text{since } L_f \leq^{P}_{m} f(U) \text{ via } \phi_{i_0}) \\ &\leftrightarrow \phi_{i_0}(\langle i_0, x\rangle) \in X && (\text{since } f(U) = X \cap f(\Sigma^*) \text{ and } \phi_{i_0}(\langle i_0, x\rangle) \in f(\Sigma^*)). \end{aligned}$$

Hence, for all x such that $n_0 \leq |\langle i_0, x\rangle|$, the function $g_1 \overset{\text{def}}{=} \lambda x.\phi_{i_0}(\langle i_0, x\rangle)$ works as a reduction from U to X.

Let π be a padding function for U. From the conditions of padding functions, we can assume an integer n_1 that satisfies the following:

$$(\forall x \in \Sigma^*)[n_0 \leq |\langle i_0, \pi(\langle x, 0^{n_1}\rangle)\rangle|] \wedge (\forall x \in \Sigma^*)[x \in U \leftrightarrow \pi(\langle x, 0^{n_1}\rangle) \in U].$$

Hence, $g_2 \overset{\text{def}}{=} \lambda x.\phi_{i_0}(\langle i_0, \pi(\langle i_0, \pi(\langle x, 0^{n_1}\rangle)\rangle)\rangle)$ is a $\leq^{\mathrm{P}}_{\mathrm{m}}$-reduction from U to X. Furthermore, because ϕ_{i_0} is a $\leq^{\mathrm{P}}_{\mathrm{inv}}$-reduction, g_2 is a $\leq^{\mathrm{P}}_{\mathrm{inv}}$-reduction from U to X. Therefore, $U \equiv^{\mathrm{P}}_{\mathrm{iso}} X$. A contradiction. □

When we consider higher complexity classes that include co-NEXP (where $\mathrm{NEXP} \overset{\text{def}}{=} \mathrm{NTIME}(2^{\mathrm{poly}})$), we can remove the condition that $f(\Sigma^*) \in P$.

Theorem 3. *Let $\mathscr{C}$ be a reasonable complexity class such that* (i) co-NEXP$\subseteq \mathscr{C}$, *and* (ii) *$\mathscr{C}$ is closed under union. Let U be a standard complete set in $\mathscr{C}$. If there exists a non-*p*-isomorphic complete set X in $\mathscr{C}$ and if $U \leq^{\mathrm{P}}_{\mathrm{m}} X$ via some honest reduction f, then $f(U)$ is a non-*p*-isomorphic complete set in $\mathscr{C}$.*

Proof. The completeness of $f(U)$ in $\mathscr{C}$ is proved as follows. Note that f is honest and polynomial time computable; thus, $f(\Sigma^*) \in \mathrm{DTIME}(2^{\mathrm{poly}}) \subseteq \mathscr{C}$. Hence, $f(U)$ $(=X \cap f(\Sigma^*))$ is in $\mathscr{C}$. The hardness of $f(U)$, more specifically, the relation $U \leqslant_{\mathrm{m}}^{\mathrm{P}} f(U)$ is proved in the same way as the above proofs.

Following an argument similar to the one in the proof of Theorem 2, we can show that $U \not\equiv_{\mathrm{iso}}^{\mathrm{P}} f(U)$. Here we consider the following set L_f:

$$\langle i, x\rangle \in L_f \overset{\mathrm{def}}{\longleftrightarrow} |i| \cdot p_i(|\langle i, x\rangle|)^2 + q \circ p_i(|\langle i, x\rangle|) \leqslant 2^{|\langle i,x\rangle|}$$
$$\wedge [\phi_i(\langle i, x\rangle) \notin f(\Sigma^*) \vee x \in U].$$

Notice that the test $\phi_i\langle i, x\rangle) \notin f(\Sigma^*)$ can be achieved by co-NEXP-computation; hence, $L_f \in$ co-NEXP. The rest of the proof is the same and thus omitted. □

It is known [1, 7] that if a deterministic time complexity class $\mathscr{C}$ includes $\mathrm{DTIME}(2^n)$, then all complete sets in $\mathscr{C}$ are $\equiv_{1,\mathrm{h}}^{\mathrm{P}}$-equivalent (i.e., $\leqslant_{1,\mathrm{h}}^{\mathrm{P}}$-reducible to each other). From this fact, we can prove the following theorem as corollary to Theorem 3.

Theorem 4. *Let $\mathscr{C}$ be a deterministic complexity class that includes* co-NEXP, *and let U be a standard complete set in $\mathscr{C}$. If there exists a non-*p*-isomorphic complete set in $\mathscr{C}$, then we have a non-*p*-isomorphic set of the form $f(U)$ for some one-way function f.*

Proof. Let X be a non-p-isomorphic complete set in $\mathscr{C}$. Since all complete sets in $\mathscr{C}$ are $\equiv_{1,\mathrm{h}}^{\mathrm{P}}$-equivalent, $U \leqslant_{1,\mathrm{h}}^{\mathrm{P}} X$ via f. (Note that f is one-to-one, honest, and polynomial-time computable.) Then it follows from Theorem 3 that $U \not\equiv_{\mathrm{iso}}^{\mathrm{P}} f(U)$. (Note that every deterministic time complexity class is reasonable and closed under union.) Furthermore, since $U \not\leqslant_{\mathrm{inv}}^{\mathrm{P}} f(U)$, f is not polynomial time invertible; thus, f is one-way. □

Acknowledgment

The author would like to thank Professor R. Book, Professor K. Ko and the referee for their comments and suggestions that helped him to improve the presentation of this paper. He also thanks Professor P. Young for his encouragement.

References

[1] L. Berman, Polynomial reducibilities and complete sets, Ph.D. thesis, Cornell University, 1977.
[2] L. Berman and J. Hartmanis, On isomorphism and density of NP and other complete sets, *SIAM J. Comput.* **6** (1977) 305–327.

[3] D. Joseph and P. Young, Some remarks on witness functions for nonpolynomial and noncomplete sets in NP, *Theoret. Comput. Sci.* **39** (1985) 225–237.

[4] S. Kurtz, S. Mahaney and J. Royer, The structure of complete degrees, in: A. Selman, ed., *Complexity Theory Retrospective* (Springer, Berlin, 1990) 108–146.

[5] S. Mahaney, On the number of p-isomorphism classes of NP-complete sets, in: *Proc. 22nd Ann. IEEE Symp. on Foundation of Computer Science* (1981) 271–278.

[6] S. Mahaney and P. Young, Reductions among polynomial isomorphism types, *Theoret. Comput. Sci.* **39** (1985) 207–224.

[7] O. Watanabe, On one-one polynomial time equivalence relations, *Theoret. Comput. Sci.* **38** (1985) 157–165.

[8] P. Young and J. Hartmanis, Fundamental contributions to isomorphism problems, in: A. Selman, ed., *Complexity Theory Retrospective* (Springer, Berlin, 1990) 28–58.